Congress blasts Feds on cyber-terror FOIA games

July 26th, 2002

By Thomas C. Green

The Register

There was a fabulous explosion Wednesday during an otherwise typical cyberterror dog-and-pony show on the Hill when House Government Reform Subcommittee Ranking Member Jan Schakowsky (Democrat, Illinois) lost her composure during a discussion of new Freedom of Information Act (FOIA) modifications proposed by the GB Junior Administration as part of its Homeland Defense initiative.

After a couple of hours filled with warnings about widespread infrastructure vulnerabilities and exploitable bugs in numerous control systems, it came time for Critical Infrastructure Assurance Office (CIAO) Director John Tritak and National Infrastructure Protection Center (NIPC) Director Ronald Dick to make the pitch for a controversial exemption from the FOIA applying to all government records submitted by the industry.

The government has been disappointed in the amount of critical information flowing to it from the Information Sharing and Analysis Centers (ISACs) which the Clinton Administration set up for private-sector vulnerability shoptalk. Industry fears that government records of their incompetence could end up in the hands of outraged citizens and journalists, leading to an unfortunate tarnishing of the sterling reputations enjoyed by the nation's mega-corporations.

Uncle Sam would like to be told more about vulnerabilities and risks and terrorist targets in the real world out there, and is perfectly willing to gut the FOIA if that's what it takes to get brought up to speed.

Schakowsky just about had a fit on hearing this. Why, she wondered, if the terrorist threat is as real as the government claims, are we kissing big business' ass and essentially pleading with them to cooperate? Why not just force them?

"This is a time of a war on terrorism; we're calling on individuals and businesses to be patriotic," she said. "Because this is so critical to our national security, we could simply require this rather than pander to the desires of businesses to keep information secret, an item that has been on their agenda for many years."

"It astounds me that at a moment in history when transparency in business is in the headlines every day -- the need for us to know what is going on in our private sector, which has deprived

many of our citizens of their ability to retire, and employees of their retirement plans, set the stock market diving because of this lack of transparency, cooking the books -- that now we want to offer...not a narrowly-constructed exemption, but a loophole big enough drive any corporation and its secrets through," she sputtered.

"If a company wants to protect information from public view, they can dump it into the Department of Homeland Security and say, 'we don't want anyone to have access to it because it's critical information,' yet it could be something that communities need to know."

She wanted to know if the government had given businesses any assistance in dealing with sensitive data under the FOIA as it exists.

NIPC Director Ronald Dick rushed to defend the proposed amendments. "If there is a request for [trade secrets information] the industry would have to come forward and discuss in court what it had done to protect that information," he explained. "So therefore they would have to go into court and prove, I assume beyond some standard, that they had adequately protected it in the first place."

That was a bit of a slip, that bit about how the new FOIA will essentially protect information the companies haven't bothered to protect for themselves. But the government often rewards incompetence, so it's hardly surprising.

"We're talking about information that the private sector believes is sensitive and are concerned about it being disclosed," Dick continued. "And they have questions as to whether the government can adequately protect it. What we're recommending is not some broad loophole, but a measured response in the language that will provide some of the assurances that will provide better information sharing."

Schakowsky read from the Junior Administration's proposed language, making it clear that Uncle Sam is prepared to exempt from public knowledge absolutely anything that relates to infrastructure vulnerabilities in any way.

Asked why such broad language should be needed, Dick made the mistake of answering, "the private sector is concerned that if they share [vulnerability information] then it will become public, and therefore the bad guys will know it and attack them."

Schakowsky tore into the logical flaw. "So they believe that if they provide information that's critical to terrorists, this government under its current laws is just going to let that information out," she said sarcastically. "It is precisely for that reason that the existing exemptions were crafted."

Dick never quite replied to that one. It's obvious to any fool that the government would never willingly release any such information. The private sector is of course solely concerned with embarrassing revelations of how badly they're managing their security defenses, and the liabilities their publication would invite.

Schakowsky knows that Uncle Sam needs and desperately wants this data and will bend over backwards to coax it from business while steamrolling the rights of citizens to sue for it, regardless of public interests buried along the way. She had a couple of good rants; and I have to say it was refreshing to see a Member of Congress actually understand something for a change. But the government rationale is fairly well accepted on the Hill, and these days the word 'terror' works absolute magic in all political negotiations. It looks like the FOIA is set become another casualty of the war on terror.